Rec'd PCT/PTO 16 FEB 2005
PCT/NL2003/000585
10/524725

Title: Computer network protection

The invention relates to protection against unauthorized access to (copies of) files stored in a computer network.

It is known in the present situation that in order to guarantee the confidentiality of electronic documents (also referred to below as "files") codes indicating which users are allowed to open the document are stored in a file system. Thus, for instance, this code can indicate whether only the author of the file has an access right or also a group to which this author belongs, or that everyone has an access right. When a user attempts to read such a file, the control system checks whether the respective user has an access right according to the codes for the requested file. Only if this is the case, the control system allows access.

This form of access control has the drawback that it is bound to the file system. This form of access control requires that users be divided previously into different kinds.

Another form of access control is the encryption of confidential files. Only those who have at their disposal the key required for the encryption of the file can get access in this way. The advantage over access codes is that now also all content-containing copies of the file are protected wherever they are. It is a drawback, however, that each time a key and decryption are required before access to the file is possible.

For protection against computer viruses, it is known besides to make use of a so-called firewall for the transport of files to a computer system. A firewall blocks the reception of files by a computer system when the file satisfies predetermined characteristics. A firewall, however, does not serve to keep confidential selected confidential files among files sent by the computer system.

It is, inter alia, an object of the invention to provide a computer system which makes it possible to selectively limit the access to files without requiring extra measures when copies are made within the computer system and without requiring encryption.

The computer system according to the invention is defined in claim 1. The invention makes use of a gate device in a communication channel between a network domain and an external connection such as a connection to the Internet. The gate device is arranged to check for the presence of a security tag all files sent to the external connection via the communication channel. Depending on the presence or absence of this security tag, the gate device limits the free sending of the file to the external connection.

In this way, a file-selective check is performed for the access possibilities to the file outside the network domain. Within the network domain, every user has access, in principle, to the file. But out of that, the access is limited. In this way, a domain specific protection is provided. In the most extreme form, the gate device blocks the sending, depending on the presence or absence of this security tag. In principle, the invention can be applied to all forms of file sending, for instance sending as part of e-mail protocols (SMTP), as part of file transfer protocols (FTP), as part of hyperlink protocols (HTTP) or any other sort of protocol.

Preferably, all communication channels of the network domain to external connections are provided with such a gate device. In one embodiment, the gate device limits free sending of files provided with such a security tag. In this way, existing or externally received files remain freely accessible, and users can themselves ask for protection.

The invention, however, is not limited to complete obstruction. In another embodiment, for instance, the gate device automatically encrypts all files provided with a security tag when these files are sent via the communication channel. In this way, protection is offered outside the network domain by means of encryption. In yet another embodiment, the

security tag is combined with an anti-tamper code which makes it practically impossible to remove the tag.

These and other objects and advantageous aspects of the computer system according to the invention will be described in more detail with reference to the following Figures.

Figure 1 shows a computer system

Figure 2 shows a gate device

Figure 1 shows a computer system with external connections 14a, 16a. The computer system comprises a domain 10 containing a number of computers 100, 102, 104, 106, 108, which are connected with each other via connections. A part of the computers 100, 102, 104, 106, 108 is connected with communication channels 14a,b, 16a,b, which run via the external connections to further computers (not shown). Located in the communication channels 14a,b, 16a,b are gate devices 11, 12. The gate devices each preferably form part of a device which also has other security tasks such as the effectuation of a firewall etc. In use, files are stored in one or more of the computers in domain 10, which files can be read via the connections from all computers in the domain. These files can be provided with security tags. In an HTML file, the security tag could, for instance, be implemented by addition of a piece of text in the form of <SECURITY> </SECURITY>, optionally supplemented with parameters. Of course, the security tag may be supplemented in all kinds of other ways, for instance by addition of other sorts of codes, or by applying a watermark in the file. Preferably, the computer is arranged to also automatically encrypt the file or the important part thereof when applying the security tag. In this way, an extra protection is realized.

When a file is sent from a computer in the domain via one of the communication channels to one of the external connections 14a, 16a, this occurs via the gate device 11 or 12. The respective gate device 11, 12 checks the file for the presence of the security tag before sending on the file to the external connection 14a, 16a. The gate device 11, 12 sends on the file only if it does not find the security tag. Besides, the gate device 11, 12 preferably stores data on the sending of the file in a log file, at least if the sending has been obstructed. This enables the system manager to check for breaches later.

Figure 2 shows an embodiment of a gate device 11 in more detail. The gate device 11 contains a first transceiver 20 for the local part of the communication channel 14b, a second transceiver 22 for the external connection 14a, a memory 24 and a tag detector 26. Transceivers 20, 22 are coupled to the memory 24. The detector 26 has an input coupled to the first transceiver 20 for the local part of the communication channel 14b and an output coupled to the second transceiver 22 for the external connection 14a.

In operation, the first transceiver 20 receives messages from the local part of the communication channel 14b and stores these messages temporarily in the memory 24. The detector 26 examines the content of the message for the presence of a file containing a security tag and sends, depending on a result of that examination, a command to the second transceiver 22. When the command purports to pass the message, the second transceiver 22 reads the message from the memory 24 and sends the message to the external connection 14a. When the message is not sent on, the message is removed from the memory 24, for instance by overwriting it with a later message without sending on the message.

The computers in the domain 10 are arranged to read or copy the respective files without a check on the security tag on all computers in the domain. In this way, it is possible to store and copy files in the domain 10 in

arbitrary places, but undesired or accidental sending to external connections 14a,b outside the domain is made impossible.

Without departing from the principle of the invention, all kinds of other embodiments are, of course, possible. Thus, for instance, the gate device 11, 12 may exactly not send on the file when no security tag is present. As a result, a user may deliberately choose to protect a file from sending.

As part of the protection, a tamper protection may be included such as, for instance, a code encrypted with a private key, which code can be decrypted with a public key and contains a number which is a function of the content of the file including the security tag. Before sending the file, the gate device may again calculate the code, then, on the basis of the file and compare with the code following from the file by public key decryption. In this way, it is ensured that the security tag cannot be changed. Also, the tag can be included in specific sorts of files as a watermark.

Furthermore, the gate device 11, 12, instead of not sending the file, may encrypt the file before sending it when the security tag indicates that free sending is not allowed. If desired, it may even be indicated with parameters in the security tag which action (for instance not sending or sending encryptedly) the file must undergo when passing the gate device 11, 12.